**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF VIRGINIA**
**Richmond Division**

| | |
|---|---|
| SYNOPSYS, INC., | |
| Plaintiff, | |
| v. | Case No. 3:21cv00252 |
| RISK BASED SECURITY, INC., | JURY TRIAL DEMANDED |
| Defendant. | |

# COMPLAINT

Plaintiff Synopsys, Inc. ("Synopsys"), for its Complaint against Defendant Risk Based Security, Inc. ("RBS"), hereby alleges as follows:

## NATURE OF THE ACTION

1. This is a declaratory judgment action arising under the copyright laws of the United States, title 17 of the United States Code. This action seeks a declaration that Synopsys does not infringe any copyright held by RBS.

2. This is a declaratory judgment action arising under the Defend Trade Secret Act, 18 U.S.C. § 1836, and the Virginia Trade Secrets Act. This action seeks a declaration that Synopsys has not misappropriated any RBS trade secret and is not liable for trade secret misappropriation under the Defend Trade Secrets Act and the Virginia Trade Secrets Act.

3. RBS has claimed and continues to claim that Synopsys misappropriated RBS trade secrets purportedly related to a database detailing vulnerabilities in open source and commercial software, which RBS calls "VulnDB." But these purported trade secrets consist of information that has been made publicly available and/or are based on publicly available information and the work of others. Likewise, RBS has further claimed and continues to claim

that Synopsys has committed copyright infringement of the VulnDB database, but RBS's assertions are baseless. Synopsys has not copied or misappropriated any of RBS' purported intellectual property because, among other things, the work purportedly subject to copyright protection is an unprotectable database, which is not an original work of authorship and does not possess any element of creativity.

4. This is an action for copyright misuse arising under the copyright laws of the United States, title 17 of the United States Code, as well as principles of equity developed under common law. This action seeks a judicial determination and declaration that RBS has engaged in unlawful copyright misuse.

5. This action also seeks a judicial determination and declaration that Synopsys has not tortiously interfered with any contract or business expectancy of RBS under Virginia law.

6. RBS has created an actual, substantial, and immediate controversy by threatening litigation over alleged copyright infringement, tortious interference, and trade secret misappropriation and by demanding that Synopsys cease and desist in lawful behavior. RBS's threats have created an actual, substantial and immediate controversy over the rights and other legal relationship between the parties, and judicial declarations confirming that Synopsys' conduct is lawful are necessary and appropriate.

## PARTIES

7. Plaintiff Synopsys is a Delaware corporation and has its principal place of business at 690 East Middlefield Road, Mountain View, California 94043.

8. Upon information and belief, Risk Based Security, Inc. is a Delaware corporation and has its principal place of business at 3308 W. Clay St., Richmond, VA, 23230-4604 and its registered agent at 5518 Olde Hartley Way, Glen Allen, Virginia 23060.

## JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1338, and 2201 because this action arises under the laws of the United States, including 17 U.S.C. §§ 101, *et seq.*; and 18 U.S.C. § 1836(c). This Court has supplemental jurisdiction over the remaining claims asserted herein pursuant to 28 U.S.C. § 1367 because they arise from the same nucleus of operative facts as the federal claims.

10. A substantial, immediate, and real controversy exists between the parties concerning the rights and legal relations of the parties, warranting the issuance of a declaratory judgment. RBS has threatened a lawsuit and taken other action to disparage Synopsys and harm its ability to compete.

11. This Court has personal jurisdiction over RBS because it resides in Virginia as RBS has its principal office in Richmond, Virginia.

12. Venue is proper in this District and Division pursuant to 28 U.S.C. § 1391 and Local Rule 3(C) because Defendant RBS resides in this District and Division and because a substantial part of the events or omissions giving rise to the claims occurred in this District and Division.

## FACTUAL BACKGROUND

### Synopsys Is a Leader in Open Source Software Security

13. Open source software—software with source code that is available for anyone to inspect, modify, and enhance—is widely used and serves as the foundation for software applications across every industry. Open source software is so prevalent that many software code owners are not aware of all the open source components in their software. Synopsys provides solutions to customers to help them identify and manage the open source components in their software.

14. As the use of open source has grown, unfortunately so has the number of vulnerabilities. A vulnerability is a weakness that can be exploited by a cyber-attack to gain unauthorized access to, or perform unauthorized actions on, a computer system. As the number of vulnerabilities grows, more and more software is at risk across every industry, including healthcare, retail and e-commerce, and education. Because open source is so widely used, it is a prime target for hackers as exploiting a single open source vulnerability can give hackers the keys to thousands of applications.

15. Synopsys is a leader in open source software security and is committed to bolstering the security of the software ecosystem. Synopsys has strived to improve the security posture of the open source community through testing tools like its Coverity Scan product and responsibly disclosing vulnerabilities it discovers in order to provide timely vulnerability information to the public.

**RBS's Vulnerability Database Product Is Based On Publicly Available and Generally Known Information**

16. RBS's primary product is a vulnerability database called VulnDB. Vulnerability databases typically contain information about known computer security vulnerabilities and users of vulnerability databases can use that information to help identify vulnerabilities that may affect their computer systems.

17. There are many vulnerability databases available on the market. For example, the U.S. National Vulnerability Database is a vulnerability database with over 100,000 records that is accessible via the World Wide Web and is freely available to all, without any confidentiality restrictions on the information contained in the database. There are a number of other vulnerability databases that are similarly accessible via the World Wide Web and freely available to all, such as the X-Force database, VulDB, and Vulners. These free, publicly available

vulnerability databases not only contain information about vulnerabilities, but also about the sources where information on those and other vulnerabilities can be found.

18. Vulnerability databases collect and aggregate information about vulnerabilities from a variety of publicly available sources, such as the MITRE repository of Common Vulnerabilities and Exposures (CVEs), blogs that discuss computer security issues, websites that focus on security issues and vulnerabilities, mailing lists, and other vulnerability databases.

19. For example, Bugtraq, Full-Disclosure, and Open Source Security mailing lists are available to anyone who wishes to be added to the mailing list. Archives of these mailing lists and others are also publicly available via the SecLists.Org Security Mailing List Archive. These and other mailing lists serve as sources for vulnerability disclosures and individuals who disclose vulnerability information often send vulnerability disclosures to multiple mailing lists or other sources for vulnerability disclosures.

20. By way of further example, vulnerability information is also available on publicly accessible websites. For example, in addition to seclists.org, various websites, such as https://packetstormsecurity.com/, https://github.com, and https://bugs.chromium.org/hosting/, make information about security vulnerabilities readily available to the public. These sources of security vulnerabilities are well known to those in the security community.

21. The Open Sourced Vulnerability Database ("OSVDB") was an open-sourced vulnerability database project that started in 2002 and officially launched to the public on March 31, 2004. The OSVDB database, which was freely accessible to the public, contained information about security vulnerabilities. By 2014, the OSVDB database had broad coverage of security vulnerabilities and contained over 100,000 vulnerabilities. Members of the public contributed vulnerability information to the OSVDB database. Upon information and belief,

most or all of the information that was publicly available in the OSVDB database is contained in RBS' VulnDB database.

22. No login was required to access the OSVDB database and there were no confidentiality restrictions or other prohibitions on non-commercial use of vulnerability information in OSVDB. The website through which the OSVDB database was accessible posted certain license terms. Those license terms did not restrict non-commercial access to or use of vulnerability information in OSVDB. Those license terms also did not restrict non-commercial sharing of vulnerability information in OSVDB, so long as OSVDB was referenced as the data source for the vulnerability information. The only prohibition imposed by the license on non-commercial access to OSVDB was a prohibition against obtaining data from the website in a programmatic fashion (such as scraping via enumeration, a web robot, or a web crawler, etc.).

23. The Open Security Foundation ("OSF") was incorporated on April 20, 2004 as a Virginia nonstock corporation. According to its Articles of Incorporation, OSF was organized exclusively for charitable, religious, educational, and scientific purposes with the specific purpose "to raise funds for the instruction of the public on subjects relating to computer security, which are useful to individuals and beneficial to the community." One of OSF's stated goals was to support OSVDB.

24. OSF recognized the public nature of sources of vulnerability information. The OSVDB license promulgated by OSF states that the information in OSVDB was "based on published vulnerability information." The OSVDB license also states that the information in OSVDB, which included sources used to identify the vulnerabilities in OSVDB, was "to be used freely."

25. OSVDB remained a free, publicly available vulnerability database between March

2004 and April 2016.

26. One of RBS's principals and founders, Jake Kouns, was one of OSF's initial directors and was the Chief Executive Officer of OSF throughout its existence.

27. In 2005, the IRS recognized OSF as a tax-exempt organization described in Section 501(c)(3) of the U.S. Tax Code. OSF represented that "OSVDB is an independent and open source database created by and for the community. Our goal is to provide accurate, detailed, current, and unbiased technical information." OSF operated as a public charity under Section 509(a)(2) of the U.S. Tax Code, meaning that it claimed public charity status and received charitable contributions that it reported to the IRS.

28. In OSF's 2010 Annual Report to the state of Virginia, Brian Martin was identified as the President and Chief Operating Officer ("COO") of OSF. Brian Martin was also one of the curators of OSVDB and now works for RBS as the Vice President of Vulnerability Intelligence.

29. RBS was formed in May 2011 by Jake Kouns and his father, Barry Kouns. RBS stated on its website that it had been established "to better support the users/contributors to the Open Security Foundation, OSF."

30. Shortly after RBS's formation, on June 2, 2011, RBS entered into an agreement with OSF to purportedly acquire all intellectual property in OSVDB, as well as an exclusive, irrevocable license to transfer, distribute, access, copy, modify, adapt, and incorporate OSVDB data into RBS products. The only consideration OSF received for the license and transfer was "management resources, funding, and capital" to continue its work on the database that RBS was purportedly acquiring.

31. Despite the fact that OSF is a 501(c)(3) non-profit organization of which Jake Kouns is the CEO and a director, and the fact that Jake Kouns was a founder of and had an

interest in RBS at the time of the June 2, 2011 agreement, he signed the June 2, 2011 agreement on behalf of OSF. Barry Kouns, Jake Kouns' father, signed the agreement on behalf of RBS.

32. Although OSF knew it had purportedly assigned any intellectual property in OSVDB to RBS, and, upon information and belief, that RBS intended to discontinue public access to OSVDB at some point, OSF continued to tout OSVDB as an open-sourced collaboration and seek and obtain contributions of vulnerability information from the public under the guise that contributions were being made to a non-profit and would be compiled into OSVDB, which would remain freely available to the public.

33. After entering into the June 2, 2011 agreement, RBS took the data in the OSVDB database, which was publicly available and had been collected through, among other methods, the voluntary contributions of third parties, and used that data as the starting point for its VulnDB product. Upon information and belief, for the next almost 5 years, OSVDB remained publicly accessible and RBS publicly shared certain VulnDB data via OSVDB.

34. On April 5, 2016, without any advance notice, RBS shut down public access to OSVDB. The VulnDB product includes data that was publicly available via OSVDB prior to April 5, 2016. On information and belief, the VulnDB product also includes contributions to OSVDB that had been made by volunteers to OSF and OSVDB both prior to the June 2, 2011 agreement between OSF and RBS and after that agreement. RBS and OSVDB personnel have given presentations and publicly posted on the web about sources for security vulnerability information. For example, in 2014, Brian Martin authored a blog post on blog.osvdb.org that discusses the Bugtraq, Full-Disclosure, Open Source Security and VulnWatch mailing lists as sources of vulnerability information. By way of further example, in 2005, Jake Kouns and Brian Martin gave a presentation titled "Vulnerability Databases: *Everything is Vulnerable*" in which

they discussed sources where vulnerability information is usually gathered. That presentation mentioned mailing lists such as Bugtraq and Full-Disclosure, as well as vendor advisories and web archives, as sources of vulnerability information for vulnerability databases.

**RBS Baselessly Accuses Synopsys of Violating its Intellectual Property Rights and Has Created an Immediate, Substantial, and Real Controversy**

35. As noted above, Synopsys has strived to improve the security posture of open source computer software. For example, it has provided the computer software community testing tools to enable detection and identification of software vulnerabilities and has responsibly disclosed through the CVE (Computer Vulnerabilities and Exposures) Program and through authorized CVE Numbering Authorities ("CNAs") vulnerabilities it discovered through its own research, which then can be remediated by other interested parties.

36. The CVE Program is an international, community-based program whose mission is to identify, define, and catalogue publicly disclosed cybersecurity vulnerabilities. "CVE IDs" are identifying means for such vulnerabilities, and under the Program, only CNAs are authorized and entrusted to assign CVE IDs to newly discovered vulnerabilities and publish information about the vulnerabilities to the CVE public catalogs.

37. Recently, in March 2021, as a result of its good stewardship of the open source software community, Synopsys was named a CNA. This unique recognition by the CVE Program authorizes Synopsys to assign CVE IDs to vulnerabilities affecting products. Synopsys joins other authorized commercial entities such as Linux, Red Hat, Google, and Microsoft as a CNA, adding to its well-regarded reputation as a recognized leader in computer software and application security.

38. RBS took issue with Synopsys being named a CNA and now seeks to prevent Synopsys from performing its authorized and trusted duties as a CNA. Specifically, on April 5,

2021, RBS sent a letter to Synopsys alleging that if Synopsys were to assign CVE IDs to newly discovered vulnerabilities and publish information about the vulnerabilities to the CVE public catalogs (the authorized functions of a CNA), such conduct would constitute trade secret misappropriation and infringe RBS' purported intellectual property rights. Ex. 1 (Apr. 5, 2021 RBS letter).

39. RBS presumes, without basis, that any CVE IDs Synopsys might locate and publish as a CNA would necessarily infringe or otherwise misuse RBS' purported intellectual property. According to RBS, the "only way" that Synopsys can supplement the CVE catalog "is by releasing information that Synopsys . . . has misappropriated from RBS's VulnDB database." Ex. 1. RBS alleges in particular that such actions by Synopsys would constitute "copyright infringement of the VulnDB database," "misappropriation of [trade secrets] under the Defend Trade Secrets Act, 18 U.S.C. § 1836 *et seq.*, and state law under the Virginia Trade Secrets Act, § 59.1-336 *et seq.*," and "tortious interference with RBS's current and prospective economic relationships under Virginia common law." Ex. 1. RBS's April 5, 2021 letter concludes by threatening "costly and time-consuming litigation" against Synopsys. Ex. 1.

40. Contrary to RBS's allegations, Synopsys uses its own cybersecurity research and its own independent access to the wealth of publicly available information concerning vulnerabilities to develop information about vulnerabilities and assign CVE identification numbers to newly discovered vulnerabilities as a CNA. It is neither misappropriating trade secrets nor infringing on any copyright.

## COUNT I

### Declaratory Judgment of No Copyright Infringement by Synopsys

41. Synopsys restates and incorporates by reference each of the allegations set forth in paragraphs 1 through 40 above, as if fully set forth herein.

42. This claim arises under the copyright laws of the United States, 17 U.S.C. § 101 *et seq.* and the Declaratory Judgment Act, 28 U.S.C. §§ 2201 and 2202.

43. There is a real, immediate, substantial, and justiciable controversy between Synopsys and RBS concerning whether Synopsys' conduct as a CNA (*e.g.*, assigning CVE IDs to vulnerabilities affecting software and disclosing such vulnerabilities to the public, including via the CVE Program's publicly accessible catalog) infringes any copyright RBS purportedly has in its VulnDB database. Synopsys agreed to fulfill the duties of a CNA and has publicly made representations that it will do so. Synopsys faces both irreparable harm in reputation and financial losses if RBS files a lawsuit for copyright infringement as a result of Synopsys fulfilling those duties, or even if it continues alleging that Synopsys' conduct as a CNA infringes copyrights.

44. This controversy is amenable to specific relief through a declaration of noninfringement, which would clarify the rights and legal relations of the parties concerning the ongoing and future conduct.

45. RBS does not own any valid and enforceable copyright in the VulnDB database. The database contents are not copyrightable subject matter under 17 U.S.C. § 102. The VulnDB database contents are not original works of authorship because, among other reasons, they are not sufficiently creative.

46. The VulnDB database is akin to a phone directory listing, but instead of listing phone numbers, it lists known cybersecurity vulnerabilities. The list contains publicly available information and information from disparate sources outside of RBS. For example, the VulnDB database includes data that was publicly available via OSVDB prior to April 5, 2016. On information and belief, the VulnDB database also includes contributions that had been made by

volunteers to OSF and OSVDB. The database content does not reflect an original work of authorship or creativity by RBS that would entitle RBS to copyright protection.

47. RBS and OSVDB personnel have given presentations and publicly posted on the web about sources for security vulnerability information. For example, in 2014, RBS employee Brian Martin authored a blog post on blog.osvdb.org that discusses the Bugtraq, Full-Disclosure, Open Source Security and VulnWatch mailing lists. By way of further example, in 2005, RBS employees Jake Kouns and Brian Martin gave a presentation titled "Vulnerability Databases: *Everything is Vulnerable*" in which they discussed sources where vulnerability information is usually gathered. That presentation mentioned mailing lists such as Bugtraq and Full-Disclosure, as well as vendor advisories and web archives, as sources of vulnerability information for vulnerability databases. Upon information and belief, the VulnDB database merely compiles listed vulnerabilities originally located through and disclosed in these type of disparate sources.

48. Even if the VulnDB database were protectable by copyright (it is not), RBS has not registered the VulnDB database or any elements or portions of the database for copyright protection pursuant to the copyright statute.

49. Even if RBS had valid copyright registrations for the VulnDB database (it does not), Synopsys' accused conduct does not infringe any of the exclusive rights afforded to a copyright owner under 17 U.S.C. § 106. For example, Synopsys does not reproduce or distribute copies of the VulnDB database.

50. Further, RBS does not own intellectual property rights in material that was contributed to OSVDB and reproduced in the VulnDB because, upon information and belief, there was no signed writing pursuant to 17 U.S.C. § 204 transferring copyright ownership from the contributors to OSF or RBS.

51. Pursuant to the foregoing, Synopsys is entitled to a judicial declaration of noninfringement for any purported RBS copyright on the VulnDB database to preserve its rights, defend its good name and protect is business and business relationships.

## COUNT II

**Declaratory Judgment of No Trade Secret Misappropriation By Synopsys, Defend Trade Secrets Act (18 U.S.C. §§ 1831–39) and Virginia Uniform Trade Secrets Act (Va. Code § 59.1-336 et seq.)**

52. Synopsys restates and incorporates by reference each of the allegations set forth in paragraphs 1 through 51 above, as if fully set forth herein.

53. RBS claims to be the owner of trade secrets contained in its VulnDB database but has refused to articulate what its alleged trade secrets are with any level of particularity, obscuring the identity of its alleged trades secrets, while simultaneously accusing Synopsys of misappropriating its purported trade secrets.

54. In doing so, RBS has created a real, immediate, substantial, and justiciable controversy between Synopsys and RBS as to whether RBS' alleged trade secrets are valid, protectable and/or misappropriated, including whether Synopsys' conduct as a CNA (*e.g.*, in assigning CVE IDs to vulnerabilities affecting products and disclosing such vulnerabilities to the public, including via the CVE Program's publicly accessible catalog) constitutes trade secret misappropriation under the Defend Trade Secrets Act and the Virginia Uniform Trade Secrets Act. Synopsys has agreed to fulfill the duties of a CNA and has publicly made representations that it will do so. Synopsys faces both irreparable harm in reputation and financial losses if RBS files a lawsuit for misappropriation of trade secrets as a result of Synopsys fulfilling those duties, or even if it continues alleging that Synopsys' conduct as a CNA misappropriates trade secrets.

55. This controversy is amenable to specific relief through a declaration of no valid or protectable trade secrets and no misappropriation, which would clarify the rights and legal

relations of the parties concerning the ongoing and future conduct.

56. None of RBS' alleged trade secrets qualify for protection under the Defend Trade Secrets Act or the Virginia Uniform Trade Secrets Act. Among other things, RBS' alleged trade secrets were not created or developed by RBS; are the subject of public knowledge and/or known to those in the field (including RBS touting that the VulnDB database comprises information that is public, widely distributed, easily accessible or discernable, and well-known within the cybersecurity and open source community); were disclosed to others (either intentionally or through RBS' failure to take reasonable measures to protect them), do not derive independent economic value, actual or potential, from not being generally known to the public or to other persons and/or were readily ascertainable by others in the field.

57. For example, the VulnDB database includes data that was publicly available via OSVDB prior to April 5, 2016. On information and belief, the VulnDB database also includes contributions that had been made by volunteers to OSF and OSVDB.

58. RBS and OSVDB personnel have given presentations and publicly posted on the web about sources for security vulnerability information. For example, in 2014, Brian Martin authored a blog post on blog.osvdb.org that discusses the Bugtraq, Full-Disclosure, Open Source Security and VulnWatch mailing lists. By way of further example, in 2005, Jake Kouns and Brian Martin gave a presentation titled "Vulnerability Databases: *Everything is Vulnerable*" in which they discussed sources where vulnerability information is usually gathered. That presentation mentioned mailing lists such as Bugtraq and Full-Disclosure, as well as vendor advisories and web archives, as sources of vulnerability information for vulnerability databases. Upon information and belief, the VulnDB database merely compiles listed vulnerabilities originally disclosed in these type of disparate sources.

59. This type of information is readily ascertainable by those in the open source and cybersecurity community. The aforementioned mailing lists manifest this, as they are community-shared publications detailing the types of vulnerabilities that are listed on VulnDB. Authors of such mailing lists and regularly skilled persons in this field can detect and identify vulnerabilities like what are listed on VulnDB by using known software tools that scan public online sources. Therefore, because the information on VulnDB is readily ascertainable, it does not derive independent economic value from not being generally known and is not a trade secret.

60. Even if RBS had valid and protectable trade secrets related to the VulnDB database (it does not), they were not misappropriated by Synopsys because they were not obtained and/or disclosed by any improper means, and Synopsys and its employees used independent research and development, public knowledge and their own innovations to create Synopsys' business, technology and products. Accordingly, Synopsys' accused conduct does not constitute misappropriation or any unauthorized conduct under the Defend Trade Secrets Act or the Virginia Uniform Trade Secrets Act.

61. Because an actual controversy exists as to the purported existence, validity and enforceability, and misappropriation of RBS' alleged trade secrets, Synopsys is entitled to, and has an immediate need for, a judicial declaration of no trade secret misappropriation under the Defend Trade Secrets Act and the Virginia Uniform Trade Secrets Act to preserve its rights, defend its good name and protect is business and business relationships.

## COUNT III

### Copyright Misuse

62. Synopsys restates and incorporates by reference each of the allegations set forth in paragraphs 1 through 61 above, as if fully set forth herein.

63. RBS is engaging in anticompetitive behavior by threatening baseless litigation

against Synopsys. RBS's threat to sue for copyright infringement is an attempt to restrain lawful Synopsys conduct based on feigned copyright rights. RBS does not own any copyright rights in the VulnDB database or its contents. The database contents are not copyrightable subject matter under 17 U.S.C. § 102, because, among other things, they are not sufficiently creative.

64. The VulnDB database is akin to a phone directory listing, but instead of listing phone numbers, it lists known cybersecurity vulnerabilities. The list contains publicly available information and information from disparate sources outside of RBS. For example, the VulnDB database includes data that was publicly available via OSVDB prior to April 5, 2016. On information and belief, the VulnDB database also includes contributions that had been made by volunteers to OSF and OSVDB. The database content does not reflect any original work of authorship or creativity by RBS that would entitle RBS to copyright protection.

65. RBS and OSVDB personnel have given presentations and publicly posted on the web about sources for security vulnerability information. For example, in 2014, Brian Martin authored a blog post on blog.osvdb.org that discusses the Bugtraq, Full-Disclosure, Open Source Security and VulnWatch mailing lists. By way of further example, in 2005, Jake Kouns and Brian Martin gave a presentation titled "Vulnerability Databases: *Everything is Vulnerable*" in which they discussed sources where vulnerability information is usually gathered. That presentation mentioned mailing lists such as Bugtraq and Full-Disclosure, as well as vendor advisories and web archives, as sources of vulnerability information for vulnerability databases. Upon information and belief, the VulnDB database merely compiles listed vulnerabilities originally disclosed in these type of disparate sources.

66. Even if the VulnDB database were protectable by copyright (it is not), RBS has not registered the VulnDB database or any elements or portions of the database for copyright

protection pursuant to the copyright statute.

67. Even if RBS had valid copyright registrations for the VulnDB database (it does not), Synopsys' accused conduct does not infringe any of the exclusive rights afforded to a copyright owner under 17 U.S.C. § 106. For example, Synopsys does not reproduce or distribute copies of the VulnDB database.

68. Despite not having any valid copyright rights, RBS has threatened that it will sue Synopsys for copyright infringement. RBS's goal is to restrain Synopsys from using material over which the RBS itself has no rights and prevent Synopsys from performing its authorized duties as a CNA (*e.g.*, in assigning CVE IDs to vulnerabilities affecting products and disclosing such vulnerabilities to the public, including via the CVE Program's publicly accessible catalog), which constitutes copyright misuse.

## COUNT IV

### Declaratory Judgment of No Tortious Interference with Existing Contract or Business Expectancy

69. Synopsys restates and incorporates by reference each of the allegations set forth in paragraphs 1-68 above, as if fully set forth herein.

70. RBS claims to have current and prospective economic relationships under Virginia common law, but has not articulated what those economic relationships are or how Synopsys acting as a CNA would tortiously interfere with those purported relationships, while simultaneously accusing Synopsys of tortious interference with RBS' current and prospective economic relationships.

71. In doing so, RBS has created a real, immediate, substantial, and justiciable controversy between Synopsys and RBS as to whether Synopsys has tortiously interfered with RBS' alleged current and prospective relationships, including whether RBS has a valid contract

or a business expectancy with a reasonable certainty of being realized, whether Synopsys had knowledge of either the contract or the expectancy, whether Synopsys' conduct as a CNA (*e.g.*, in assigning CVE IDs to vulnerabilities affecting products and disclosing such vulnerabilities to the public, including via the CVE Program's publicly accessible catalog) intentionally interferes with the contract or the expectancy, and whether RBS has suffered any resultant damage. Synopsys has agreed to fulfill the duties of a CNA and has publicly made representations that it will do so. Synopsys faces both irreparable harm in reputation and financial losses if RBS files a lawsuit for tortious interference with RBS's current or prospective economic relationships as a result of Synopsys fulfilling those duties, or even if it continues alleging that Synopsys' conduct as a CNA tortiously interferes with RBS' business relationships.

72. This controversy is amenable to specific relief through a declaration of no knowledge by Synopsys of any RBS contract or business expectancy, no employing of improper means or methods by Synopsys to intentionally interfere with any RBS contract or business expectancy, and no damage to RBS as a result of Synopsys acting as a CNA, which would clarify the rights and legal relations of the parties concerning their ongoing and future conduct.

73. Even if RBS had valid contracts or business expectancies with a reasonable certainty of being realized, Synopsys had no knowledge of those relationships. And even if Synopsys did have such knowledge (it did not), acting as a CNA would not impact those relationships. In addition, Synopsys has not employed improper means or methods in acting as a CNA and therefore has not intentionally interfered with any RBS contract or business expectancy. Accordingly, Synopsys' accused conduct does not constitute tortious interference with a current or prospective business relationship under Virginia law.

74. Because an actual controversy exists as to the purported existence, and Synopsys'

knowledge, of any RBS contract or business expectancy, and whether Synopsys employed improper means or methods to intentionally interfere with any RBS contract or expectancy, Synopsys is entitled to, and has an immediate need for, a judicial declaration of no tortious interference with a current or prospective business relationship under Virginia law to preserve its rights, defend its good name and protect is business and business relationships.

**PRAYER FOR RELIEF**

WHEREFORE, Synopsys respectfully prays for judgment in favor of Synopsys and against RBS, as follows:

A) for a judicial determination and declaration that Synopsys has not infringed any copyright belonging to RBS;

B) for a judicial determination and declaration that Synopsys has not misappropriated any trade secret belonging to RBS under either the Defend Trade Secrets Act or the Virginia Uniform Trade Secrets Act;

C) for a judicial determination and declaration that RBS has engaged in unlawful copyright misuse;

D) for a judicial determination and declaration that Synopsys has not tortiously interfered with an existing contract or business expectancy under Virginia law;

E) for damages;

F) for reasonable attorneys' fees and costs incurred in this suit as allowed by law and agreement of the parties; and

G) for such other relief as the Court deems just and proper.

## DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff hereby requests a trial by jury of all issues so triable.

Dated: April 14, 2021

Respectfully submitted,

OF COUNSEL:
Krista S. Schwartz (PHV forthcoming)
Patrick T. Michael (PHV forthcoming)
HOGAN LOVELLS US LLP
3 Embarcadero Center, Suite 1500
San Francisco, CA 94111
Phone: (415) 374-2300
krista.schwartz@hoganlovells.com
patrick.michael@hoganlovells.com

*/s/ Christopher T. Pickens*
N. Thomas Connally, VSB No. 36318
Christopher T. Pickens, VSB No. 75307
HOGAN LOVELLS US LLP
8350 Broad St., 17th Floor
Tysons, VA 22102
T: 703-610-6100
F: 703-610-6200
tom.connally@hoganlovells.com
christopher.pickens@hoganlovells.com

*Attorneys for Plaintiff Synopsys, Inc.*